UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,610	05/31/2001	Dwip N. Banerjee	AUS9-2001-0361-US1	1787

40412 7590 09/22/2005

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
BAYARD, DJENANE M	
ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/870,610	**Applicant(s)** BANERJEE ET AL.
	Examiner Djenane M. Bayard	**Art Unit** 2141

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,7-9,11,13,14,18 and 20-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,7-9,11,13,14,18 and 20-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Allowable Subject Matter

1. The indicated allowability of claims 1,8 14 and 27 is withdrawn in view of the newly discovered reference(s) to U.S. Patent No. 6,636972 to Ptacek et al. Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1, 8 and 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant failed to provide a description for "client data area" in the specification.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 14, 18, 25 and 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The computer program product for preventing malicious network attacks of claims 14, 18, 25 and 26 is non statutory as not being tangible embodied in a manner so as to be executable.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 5, 8, 11, 14 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent Application No. 2002/0101819 to Goldstone and further in view of U.S. Patent No. 6,189035 to Lockhart et al.

a. As per claims 1, 8 and 14, Gupta et al teaches a method for preventing malicious network attacks said method comprising: receiving a packet from a client computer (See col. 7, lines 35-37); calculating a number of packets received using the source IP address during a time interval (See col. 7, lines 42-44, The number of packets received from the source during the predetermined time period is determined). However, Gupta et al fails teach wherein the calculating includes: identifying a client data area based on the source IP address, the client data area including the number of packets received; and incrementing the number of packets received; comparing the number of packets received with one or more configuration settings; determining an action from a plurality of actions based on the comparing'; and executing the action (See col. 7, lines 46-47, the router discards the packet if the rate limit has been exceeded)

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore, Godlstone teaches wherein the client computer is identified by a source IP address (See page 3, paragraph [0039]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the client computer is identified by a source IP address as taught by Goldstone in the claimed invention of Gupta et al in order to deny future request to connect that are initiated from an attacking client (See page 3, paragraph [0039]). However, Gupta et al in view of Goldstone fails to teach wherein the calculating includes: identifying a client data area based on the source IP address, the client data area including the number of packets received; and incrementing the number of packets received.

Lockhart et al teaches a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets. In the next step 60, that recent packet count for the present IP source is incremented by one. (18). The present process also maintains a count representing the count of all data packets received. (See col. 3, lines 65-67 and col. 4, lines 1-50).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the calculating includes: identifying a client data area based on the source IP address, the client data area including the number of packets received; and incrementing the number of packets received as taught by Lockhart et al in the claimed invneiton of Gupal in view of Goldstone in order to limit to a number which the internal network can handle the number of incoming packet without unduly degrading its operation 9See col. 2, lines 51-56).

c. As per claims 5, 11 and 18, Gupta et al in view of Golsdsotne and further in view of Lockhart et al teaches the claimed invention as described above. However, Gupta et al failed to teach receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison.

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore,. Godlstone teaches receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison (See page 3, paragraph [0038]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison as taught by Goldstone in the claimed invention of Gupta et al in order for the router to prevent the attacking client from perpetrating further attacks by blocking traffic originating from the attacking client from entering the Internet (See page 3, paragraph [0027]).

8. Claims 7, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent Application No. 2002/0101819 to Goldstone and further in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claim 1, 8 and 14 above, and further in view of U.S. Patent No. 5,892,903 to Klaus.

a. As per claims 7, 13 and 20, Gupta et al in view of Goldstone and further in view of Lockhart et al teaches the claimed invention as described above. However, Gupta et al in view of Goldstone failed to teach providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination.

Klaus teaches a method and apparatus for detecting and identifying security vulnerabilities in an open network computer communication system. Furthermore, Klaus teaches providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination (See col. 9, lines 1-41)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination as taught by Klaus in the claimed invention of Gupta et al in view of Goldstone and further in view of Lockhart et al in order to detect which computers on a network are susceptible to attacks using predicted TCP sequence numbers (See col. 6, lines 15-20).

9. Claims 21, 23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent Application No. 2002/0101819 to Goldstone and further in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claim 1, 8 and 16 above and further in view of U.S. Patent No. 6,381649 to Carlson.

a. As per claim 21, 23 and 25, Gupta et al in view of Goldstone and further in view of Lockhart et al teaches the claimed invention as described above. However, Gupta et al in view of Goldstone and further in view of Lockhart et al fails to teach wherein configuration settings include a first limit and a second limit, the method further comprising: determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

Carlson et al teaches determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit (See col. 7, lines 55-67 and col. 8, lines 1-8)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit as taught by Carlson in the claimed invention of Gupta et al in view of Goldstone and further in view of Lockhart et al in order to monitor or police data traffic 9See col. 1, lines 61-64).

10. Claims 22, 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent Application No. 2002/0101819 to Goldstone and further in view of U.S. Patent No. 6,189035 to Lockhart et al as applied to claim 1, 8 and 16 above and further in view of U.S. Patent No. 6,321338 Porras et al.

a. As per claim 22, 24 and 26, Gupta et al in view of Goldstone and further in view of Lockhart et al teaches the claimed invention as described above. However, Gupta in view of Goldstone and further in view of Lockhart et al fails to teach wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage.

Porras et al teaches wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage (See col. 6 and 7); and sending a notification in response to determining that the number of packets is higher than the historical usage (See col. 2, lines 54-56).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage as taught by Porras et al in the claimed invention of Gupta et al in view of Goldstone and further in view of Lockhart et al in order to identify attacks causing disturbances in more than one network entity 9See col. 2,lines 58-60).

11. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,636972 to Ptacek et al in view of U.S. Patent No. 6,189035 to Lockhart et al and further in view of U.S. Patent Application No. 2002/0059454 to Barrett et al.

a. As per claim 27, Ptacek et al teaches a system and method for building an executable script for performing a network security audit. Furthermore, Ptacek et al teaches executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including (See col. 24, lines 30-42): receiving, at the server computer, one or more packets from the client computer and one or more open socket requests from the client computer (See col. 26, lines 25-37) and the evaluating including: analyzing the performance of the server computer during the simulation; and adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit (See col. 6, lines 29-53). However, Ptacek et al fails to teach deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer; computing an open socket threshold for the client computer, the computing including: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations,

Lockhart et al teaches Lockhart et al teaches a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets. In the next step 60, that recent packet count for the present IP source is incremented by one. (18). The present process also maintains a count representing the count of all data packets received... If the answer is negative, the program proceeds to step 70 where a determination is made as to whether the total packet count exceeds its threshold. If the answer is negative, the packet is negative. Otherwise, the packet is discarded. (See col. 3, lines 65-67 and col. 4, lines 1-50).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer as taught by Lockhart et al in the claimed invention of Ptacek et al in order to determine the packet loss rate calculation over a predetermined window interval (See col. 21, lines 65-67). However, Ptacek et al in view of Lockhart et al fails to teach: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations.

Barrett et al teaches determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations (See page 1, paragraph [0006]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations as taught by Barrett et al in the claimed invention of Ptacek et al in view of Lockhart et al in order to limit to a number which the internal network can handle the number of incoming packet without unduly degrading its operation 9See col. 2, lines 51-56).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Djenane M. Bayard whose telephone number is (571) 272-3878. The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Djenane Bayard

Patent Examiner

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER